CLAIMS

1. A method comprising:

randomly retrieving data from a removable data storage medium, wherein the removable data storage medium contains an executable application program;

comparing the retrieved data to corresponding verification data, wherein the verification data is known to be valid; and

allowing execution of the executable application program if the retrieved data matches the corresponding verification data.

2. A method as recited in claim 1 further including preventing execution of the executable application program if the retrieved data does not match the corresponding verification data.

3. A method as recited in claim 1 wherein the executable application program is executed from the removable data storage medium.

4. A method as recited in claim 1 wherein the executable application program is executed on a computer system performing the method.

5. A method as recited in claim 1 wherein the removable data storage medium is a compact disc (CD).

6. A method as recited in claim 1 wherein the removable data storage medium is a digital versatile disc (DVD).

7. A method as recited in claim 1 further including partitioning the removable data storage medium into a plurality of data blocks.

8. A method as recited in claim 1 further including:

partitioning the removable data storage medium into a plurality of data blocks; and

calculating a cryptographic digest for each of the plurality of data blocks.

9. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 1.

10. A method comprising:

randomly retrieving data from a removable data storage medium, wherein the removable data storage medium contains at least one file of audio data;

comparing the retrieved data to corresponding verification data, wherein the verification data is known to be valid; and

allowing access to the at least one file of audio data if the retrieved data matches the corresponding verification data.

11. A method as recited in claim 10 further including preventing access to the at least one file of audio data if the retrieved data does not match the corresponding verification data.

12. A method as recited in claim 10 wherein the removable data storage medium is a compact disc (CD).

13. A method as recited in claim 10 wherein the removable data storage medium is a digital versatile disc (DVD).

14. A method as recited in claim 10 wherein allowing access to the at least one file of audio data includes installing the at least one file of audio data to a handheld audio player.

15. A method as recited in claim 10 wherein allowing access to the at least one file of audio data includes playing the at least one file of audio data on a handheld audio player.

16. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 10.

17. A method of verifying the presence of a legitimate removable data storage medium, the method comprising:

randomly retrieving at least one data block from the removable data storage medium, wherein the removable data storage medium contains a plurality of data blocks;

comparing the retrieved data block to a corresponding verification data block, wherein the verification data block is known to be valid; and

determining that a legitimate removable data storage medium is present if the retrieved data block matches the corresponding verification data block.

18. A method as recited in claim 17 further including determining that a legitimate removable data storage medium is not present if the retrieved data block does not match the corresponding verification data block.

19. A method as recited in claim 17 wherein the removable data storage medium is a compact disc (CD).

20. A method as recited in claim 17 wherein the removable data storage medium is a digital versatile disc (DVD).

21. A method as recited in claim 17 further including calculating a cryptographic digest for each retrieved data block, wherein the verification data block has an associated cryptographic digest.

22. A method as recited in claim 21 wherein comparing the retrieved data block to a corresponding verification data block comprises comparing the cryptographic digest of the retrieved data block with the cryptographic digest associated with the verification data block.

23. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 17.

24. A verification system comprising:

a data reading device to read data from a removable data storage medium; and

a verification module coupled to the data reading device, wherein the verification module is to randomly retrieve data from the removable data storage medium and compare the retrieved data to corresponding verification data that is known to be valid, and wherein the verification module is further to determine that a legitimate removable data storage medium is present if the retrieved data matches the corresponding verification data.

25. A verification system as recited in claim 24 wherein the verification module is further to determine that a legitimate removable data storage medium is not present if the retrieved data does not match the corresponding verification data.

26. A verification system as recited in claim 24 wherein the data reading device is a compact disc read-only memory (CD-ROM) drive.

27. A verification system as recited in claim 24 wherein the data reading device is a digital versatile disc read-only memory (DVD-ROM) drive.

28. A verification system as recited in claim 24 wherein the verification module and the data reading device are coupled to one another across the Internet.

29. A verification system as recited in claim 24 wherein the verification module is located in a handheld audio player and the data reading device is located in a computer system coupled to the handheld audio player.

30. One or more computer-readable media having stored thereon a computer program comprising the following steps:

randomly retrieving data from a removable data storage medium;

comparing the retrieved data to corresponding verification data, wherein the verification data is known to be valid; and

determining that a legitimate removable data storage medium is present if the retrieved data matches the corresponding verification data.

31. One or more computer-readable media as recited in claim 30 further including the step of determining that a legitimate removable data storage medium is not present if the retrieved data does not match the corresponding verification data.

32. One or more computer-readable media as recited in claim 30 wherein the removable data storage medium is a compact disc (CD).

33. One or more computer-readable media as recited in claim 30 wherein the removable data storage medium is a digital versatile disc (DVD).

34. A method comprising:

randomly selecting a data block identifier, wherein the data block identifier identifies a particular data block on a removable data storage medium;

issuing a challenge and the data block identifier to a data reading device, wherein the removable data storage medium is readable by the data reading device;

the data reading device hashing the challenge with the data contained in the particular data block on the removable data storage medium;

receiving the result of the hashing operation;

comparing the result of the hashing operation to corresponding verification data, wherein the verification data is known to be valid; and

determining that the removable data storage medium is legitimate if the result of the hashing operation matches the corresponding verification data.

35. A method as recited in claim 34 further including determining that the removable data storage medium is not legitimate if the result of the hashing operation does not match the corresponding verification data.

36. A method as recited in claim 34 wherein the removable data storage medium is a compact disc (CD).

37. A method as recited in claim 34 wherein the removable data storage medium is a digital versatile disc (DVD).

38. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 34.